



AbstractPlus

[BROWSE](#)

[SEARCH](#)

[IEEE XPLORE GUIDE](#)

[SUPPORT](#)

[View TOC](#)

e-mail printer friendly

Access this document

Full Text: [PDF](#) (172 KB)

Download this citation

Choose [Citation & Abstract](#)

Download [ASCII Text](#)

[» Learn More](#)

Improved identity-based key sharing system for multiaddresscommunication

[Laih, C.-S.](#) [Kuo, W.-C.](#)

Dept. of Electr. Eng., Cheng Kung Univ., Tainan ;

This paper appears in: [Electronics Letters](#)

Publication Date: 17 Mar 1994

Volume: 30, Issue: 6

On page(s): 478-479

ISSN: 0013-5194

References Cited: 7

CODEN: ELLEAK

INSPEC Accession Number: 4670800

Posted online: 2002-08-06 19:28:00.0

Abstract

For the original article see *ibid.*, vol. 28, p. 1015-17 (1992). The commenters show that even though the improved ID-based key sharing system, proposed by T. Chikazawa and A. Yamagishi in the aforementioned paper, can resist the SK attack, the improved scheme as well as the original scheme can be completely broken by the conspiracy of $(n+1)$ entities with overwhelming probability

Index Terms

Indexing

Controlled Indexing

[cryptography](#) [matrix algebra](#) [probability](#)

Non-controlled Indexing

[ID-based system](#) [SK attack](#) [identity-based key sharing system](#) [key preparation](#)
[multiaddress communication](#) [trusted centre](#)

Author Keywords

Not Available

References

No references available on IEEE Xplore.

Citing Documents

No citing documents available on IEEEExplore.

[View TOC](#) | [Back to Top](#)

Indexed by
 InsPEC

[Help](#) [Contact Us](#) [Privacy & Security](#) [IEEE](#)

© Copyright 2006 IEEE – All Rights Reserved